AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

#Terror

Social Media and Extremism

By

Joshua Close, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Paul J. Springer

Maxwell Air Force Base, Alabama

May 2014

Disclaimer

The views expressed on this academic research paper are those of the author and do not reflect the official policy or position of the US Government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

Technological advances and social media are both amoral; in and of itself, there is no good social media or bad social media. Like the rest of the world, extremist organizations have discovered social media and are not going to stop using it anytime soon. Terror organizations often utilize new technology in the same manner as an everyday user. Open access in cyberspace forces countries into a paradoxical position of how to grant access to the internet yet maintain control of the social media messaging and propaganda. There are varied solutions from countries around the globe that range from invasive to innovative. These varied solutions prove there is no silver bullet to solve the problem; the United States needs to find a balanced solution to effectively police social media and maintain America's fundamental values.

INTRODUCTION

Less than six weeks ago, the Syrian extremist group Islamic State of Iraq and Syria (ISIS) took to the internet in what was a first of its kind; live tweeting the act of severing a man's hand. A group known for acts extreme enough to give Al-Qaeda pause, ISIS remarked the man would rather remove his hand than live with the sin of thievery.[1] Throughout the process, a Twitter account @reyadiraq took pictures of before, during and after the event. Twitter banned the account after the amputation took place, but at the time, the account had over 96,000 followers and had tweeted over 20,000 times.[2]

ISIS' ultimate goal is the installation of strict Islamic rule of law in Iraq and Syria. The amputation sends many messages, least of all being the depth of their dedication. Such brutality and conviction has placed the group at odds with the local Syrians. Under pressure, the group fled the northern Syrian town of Azaz earlier in the month; a cell phone video placed on YouTube shows the celebrations of the townsfolk rejoicing at the ISIS retreat.[3]

A brutal, yet simple act in the grand scheme of world affairs found its way to *Washington Post* journalists who wrote a story about it. This is the power social media has to propagate information around the globe. The article indicates that social media as a way the separate factions in the conflict processed and distributed information on the internet. ISIS utilized Twitter and the people of Azaz relied on YouTube.

Terrorist use of social media should not be surprising to anyone. Social networking existed long before the advent of Facebook, Twitter or YouTube. Social networking before the internet, as described by Evan Kohlmann in his testimony before Congress was, "the process of conventional human interaction that took place in key locations like schools, marketplaces, religious centers and sporting events."[4] Technological advances have only moved the interaction

from face-to-face to cyberspace. Extremist organizations have embraced these technological advances with fervor.

An Al-Qaeda publication attributed to Mohammad bin Ahmad Al-Salem[a] lists the 39 principles of jihad. One of the principles is, "performing electronic jihad."[5] The principle describes cybercrime and cyber vandalism against US and Israeli websites, but it also explicitly mentions the social aspect the internet provides. Al-Salem instructs Muslims to join the jihad through, "participating in internet forums to the [sic] Islam...preach Jihad...encourage Muslims to learn more about this sacred duty."[6] Al-Salem also grasps the power of the internet when he acknowledges it, "provides an opportunity to reach vast target audiences and respond swiftly to false allegations."[7]

Al Qaeda's dedication to preaching jihad on the internet is not only word, but also deed. Osama bin Laden biographer Hamid Mir noted as the group began to scatter during Operation Enduring Freedom that he saw, "every second Al Qaeda member carrying a laptop computer along with a Kalishnakov."[8] Mir made this comment in 2005 and the use of the internet by terrorist organizations has only grown since. In 1998, there were barely a dozen recognized terrorist websites. The number grew exponentially over the next decade and a half to over 6,000 websites today, not including social media.[9] What extremists initially planted as underground websites and blacklisted forums scattered throughout the internet has blossomed into mainstream use of social media spreading propaganda and recruiting new members out in the open. The internet is now the primary and preferred method of dissemination of jihadist propaganda and media activity.[10]

[a] There is no record of Mohammad bin Ahmad Al-Salem, suggesting a false identity to conceal himself from Saudi Arabian authorities

There is a reason the internet rose to the top of terrorist propaganda machines. In general, the internet, and more specifically, social media are under-regulated in a vast majority of regions around the globe. It is location independent, providing anonymity from behind a computer screen, it also allows jihadists quickly to respond to stories in the media, or create the talking points themselves. Finally, the cost ratio of social media activities is extremely low; the cost of entry is a computer and a service provider, which is free in an increasing number of places that offer public Wi-Fi access.[11]

Once on the web, there are seven basic uses the internet provides terrorist organizations: recruitment, training, communications, operations, propaganda, funding and psychological warfare.[12] Short of actually conducting physical operations, the internet provides almost everything organizations need to function. Compare how a terrorist organization uses the internet with the way any company, large or small, uses the internet, and there will be a significant overlap. Sushil Pradhan, a Lieutenant Colonel in the Indian Army adds an eighth way to use the internet, data mining, or in simpler terms, open source intelligence. He also goes on to lay out the three audiences terrorists are trying to reach through the internet, supporters (realized and potential), international public and enemy populations.[13]

Extremist organizations are embracing the new technology with open arms. Consider the following posts taken from a jihadist forum regarding Facebook usage:

> This [Facebook] is a great idea, and better than the forums. Instead of waiting for people to [come to you so you can] inform them, you go to them and teach them! God willing, the mujahedeen, their supporters, and proud jihadi journalists will [use the site, too]. [First,] it has become clear that the market of social networking websites is developing in an astonishing manner and that it fulfills important needs for Internet users, particularly younger ones. [sic][14]

Extremists have found social media and they are not going to stop using it anytime soon. There is no good social media or bad social media, technological advances and social media are both amoral. Terror organizations utilize this new technology along with the rest of the world. Open access in cyberspace forces countries into a paradoxical position of how to grant access to the internet yet maintain control of the social media messaging. There are varied solutions from countries around the globe that range from invasive to innovative. These varied solutions prove there is no silver bullet to solve the problem; the United States needs to find a balanced solution to effectively police social media and maintain America's fundamental values.

EXREMIST USE OF SOCIAL MEDIA

Each month, nearly 2 billion unique visitors view YouTube, Facebook and Twitter combined.[15] One-third of the earth's population went to one of those sites at least once in the last month. A key to the popularity of social media is the Web 2.0 infrastructure on which it rides. Web 2.0 is dynamic user driven web content, vice the previous Web 1.0 design that relied upon web designers and was relatively static. As a comparative example, Web 1.0 gives the user a painting to look at; Web 2.0 gives the user a canvass, paint and brushes. History shows terrorist organizations use each of these three websites in some form or another. Though Facebook, YouTube and Twitter all are lumped in the broad category of social media, each site has niche functions that make them popular not only to the common user, but also to the extremist.

One of the largest canvasses on the internet today is YouTube, the second most active website in the world, behind only to Google, its owner. The site alone records over 1 Billion unique visitors every month, almost a fifth of the world's population.[16] YouTube is more effective than its textual counterparts Facebook and Twitter because of its ability to incorporate audio and video for the user. Like Facebook, YouTube can touch most of the eight terrorist uses

of the internet, but the three it is most adept at are propaganda, recruitment/radicalization and training.

Probably the most well-known extremist use of YouTube is the propaganda videos prevalent throughout. Anyone with a video camera, an internet link and a YouTube account can upload videos onto the site. The Electronic Resistance, a YouTube channel dedicated to Hezbollah posts multiple videos weekly supporting the organization. A view of their channel page shows the video of a Hezbollah soldier tearing down an Israeli flag, replacing it with a Hezbollah flag and saluting while Hassan Nasrallah fades into the background stating, "...its resistance is ready."[17] The professional quality of the video and the patriotism and pride of the Hezbollah soldier are stellar examples of the type of propaganda extremist groups are capable of on YouTube.

Jihadist terror, however, is not the only type of extremism on YouTube. A quick search for the Aryan Nation reveals an entire channel dedicated to the sermons on its spiritual leader, Morris L. Gullet.[18] All the comments for his latest sermon on March 23, 2014 are approving of this known white supremacist, including a link to another organization known as the Aryan Kindred Organization.[19] In social networking, like minds and ideas gravitate towards one another and spread.

The propaganda videos lead to the second use of YouTube by extremist organizations for recruitment and radicalization. Recruitment does not solely have to be for future operatives within the organization, it occurs for any organizational role. Chechen rebels used YouTube videos to recruit donors in order to raise funds against their Russian antagonists, also demonstrating that terror activity on social media is not just against the United States and western countries.[20] An American's idea of self-radicalization looks to the case studies of MAJ

Nidal Hassan and his attack at Ft. Hood or the Tsarnaev brothers attack on the Boston Marathon. A lesser-known case study of self-radicalization from YouTube is Roshanara Choudhry, a British woman who stabbed a Member of Parliament after watching radicalizing YouTube videos.

Upset with Parliament Member Stephen Timms' vote in favor of the Iraq War, Ms Choudhry stabbed him at a community center in 2010 in order to get, "revenge for the people of Iraq."[21] After her arrest, during her interrogation she revealed her hope to become a martyr, as that was the, "best way to die."[22] The core of all her vitriol and violence came from YouTube where she admitted viewing videos from American cleric Anwar al-Awlaki. The most powerful statement Ms Choudhry gave was she had not even heard of al-Awlaki until she saw his videos, "I wasn't searching for him, I just came across him. I used to watch videos that people used to put up about like [sic] how they became a Muslim."[23] Through videos not related to terrorism, she came across Anwar al-Awlaki's sermons, became intrigued, and then radicalized to the point she attempted to assassinate a Member of Parliament. The cost of that operation to terror organizations was nil. There was no group even associated with her, but despite that fact, it does not mean Ms Choudhry was a lone wolf. Though she may have physically operated alone, she was ideologically in line with the jihad movement.[24]

Once propaganda and recruitment of a new member is complete, YouTube can train new recruits as well. The site excels at providing training and how-to guides on nearly anything imaginable. What makes the site so advantageous to terrorist groups is the innocuous nature of much of the training. A search for "how to clean an AK-47"[25] came up with dozens of videos, none of which related to anything resembling a terror organization, yet these videos teach the terrorist recruit right alongside the gun enthusiast. Further searches revealed non-operational

training available on the site. Searching, "how to fundraise money,"[26] brings up a video from CNN's Anderson Cooper promoting a best-selling author's most recent book on raising money.

The difficulty with these training videos examples is that none of them incites violence and YouTube will not remove them since they do not violate the terms of agreement.[27] Terror organizations can develop entire training programs based on what they can find on YouTube. None of the material needs to come from the organization itself. YouTube is a boon website for terror organizations, as it can push propaganda, recruit, radicalize and train.

Behind YouTube in popularity is the ever-present Facebook. Home to more than 900 million monthly viewers, Facebook is the third most visited website in the world trailing only the previously mentioned Google and YouTube.[28] Similar to other social media websites, Facebook has multiple services and products available to its users. Utilizing these products, extremist's primary use of the site is for propaganda with the intent of recruitment.[29]

Extremist groups using Facebook to attract recruits do not have to be significantly obtuse in their rhetoric. Through simple statements discrediting western and mainstream news and talking points, terrorist organizations manipulate the stories to their favor.[30] In the news culture of today, people gravitate more towards what they want to hear, rather than the facts of a story. In a book review on the death of journalism, columnist Chris Hedges writes, "[online news] has severed a connection with reality-based culture...and replaced it with a culture in which facts, opinions, lies, and fantasy are interchangeable."[31] Against online information's haze of reality, extremist groups operate with impunity.

Facebook recruitment is more akin to the frog in a boiling pot of water than a spontaneous combustion of terror sympathy. An effective recruitment starts with simply attracting a user to the group's page, regardless of reason. The user does not have to overtly

agree with terror organizations, they just need a reason to click the link. Facebook group pages do not have to complete the recruitment. To borrow terminology from drug cultures, Facebook acts as a "gateway" to sites that are extreme and radical.

As an example of how effective recruiting can be, in December 2008, members of the al-Faloja Islamic Forums instructed its members to flood Facebook, creating groups sympathetic to Jihad.[32] Al-Faloja forum members understood Facebook casts a wide net through linking "user likes" and viewed pages. Individuals would be able to see which sites their friends had gone to, and the software would recommend the Jihadist websites without an actual person having to intervene. The tactic worked. Within the month, Pakistani authorities arrested five US youth of Muslim decent, who acknowledged the groups Lashkar-e-Taiba and Lashkar-e-Jkangyi recruited them from their YouTube and Facebook websites.[33] Like many social media sites, Facebook, YouTube and Twitter have links between each site allowing quick access from one to the others and it is available 24/7/365 for anyone to find.

With Twitter however, followers do not even need to look up the site in the middle of the night, they automatically receive tweets of people they are following. The newest social media trend, Twitter is the eighth most visited website in the world, garnering 290 million unique visitors each month.[34] Similar to Facebook, individuals can follow a person, what makes Twitter unique from Facebook is the organic nature of its hashtag groups. A hashtag (#) and the words following group all tweets with the same hashtag together. Whereas a Facebook group needs to have an individual to create and maintain the page, a hashtag group is completely organic since once started the originator does not need to maintain anything and any Twitter user can contribute.[35]

Another advantage to Twitter for terrorist groups is the site's abysmal record on regulating hate speech and terror propaganda. Digital Trends website grades the site an "F" when compared against Facebook (A-) and YouTube (C) in removing offensive content.[36] Twitter does not actively monitor accounts, instead relying on outside reports to investigate violations, which are rare. Even if an account is blocked, they often reappear shortly thereafter with a different account name. As an example, the Syrian Electronic Army resurfaced over a dozen times after having their accounts banned on Twitter.[37] The ease of access and fluid nature of Twitter make it usable by terrorist organizations for multiple purposes. The standard propaganda and recruitment, but in addition Twitter is used to communication with the public and as command and control in kinetic operations.

Boko Haram, a Nigerian terror organization, undertook a bombing campaign in 2011-2012, centered on the towns of Maiduguri, Damataru, and Jos.[38] The group used Twitter during the campaign to communicate with the people of Nigeria, both supporters and antagonists. The tweets took different tones; some attacked the ineptness of the central government, "How many jets does the president have? How many jobs would that have created? Boko Haram to the rescue (#wherewedarethread)" and "The government is the terrorist. When last did you have light for 24 hrs? Boko Haram are the freedom fighters."[39] The tweets serve to deflect from their attack and focus the blame on the government; the actions of Boko Haram are for the people and would not be necessary if the government did its job correctly.

Other tweets from the group spoke to the perceived benefits of its campaign in the cities that were attacked, "Pls come to Maiduguri to see the good job we have done. Quiet. No siren. No thieves only us, polis and army. #tourism."[40] This tweet encourages its followers to visit the city it just attacked, claiming it is now safe for all. It also stretches reality to show that their

attacks have reduced the amount of drunkenness, "Rate of alcoholism has been reduced in Abuja and Maiduguri because of our good work #collateraleffect," albeit through killing those found to be intoxicated.[41] Again, Boko Haram is using Twitter to get ahead of the story, showing the positives of the attack and attempting to shift blame onto the others, asserting that the government forced their hands into the attacks they committed.

Another terror group on the African continent, Al Shabaab, also has a history of using Twitter. Most recently, the group took to Twitter to claim responsibility for the Westgate Mall attack in Kenya, the account was removed, but like the aforementioned Syrian Electronic Army, Al Shabaab had a new account and was tweeting about the attack within the day.[42] Despite their focus on the Horn of Africa, Al Shabaab made enough time to tweet on the Boston Bombings. The first tweet, harshly satirical, "Don't you just hate it when you don't reach the finish line #BostonBombings," obviously intended to raise people's angst was followed by a second, more ideological tweet, "The #BostonBombings are just a tiny fraction of what US soldiers inflict upon millions of innocent Muslims across the globe on a daily basis."[43] The group used the site and the hashtag just a day after the event to make itself relevant in a situation where it was half a world away.

Extremists have also used Twitter for operational missions. The Pakistani group Lashkar-e-Taiba attacked 10 different sites in Mumbai in 2008, killing 164 and injuring nearly twice as many.[44] What makes the attack interesting is the use of technology and Twitter to affect its success. The operational element carried Blackberry devices with multiple SIM cards in case the authorities blocked them during the operation. The command and control element outside the attack used live tweets to keep track of the situation, to include movement of Indian counter-terrorism forces, which they relayed to the attackers via Blackberry.[45] The real-time social

media feeds of the attack assisted the perpetrators to carry out the deadly operation by providing situational awareness. Lashkar-e-Taiba used Twitter no different from an individual tweeting the play-by-play of a football game they are watching in the stands.

YouTube, Facebook, and Twitter all provide simple uses for terrorist organizations, uses that are the same as everyday individuals. Whether it is recruiting through video message, creating Facebook groups to collaborate and reinforce ideologies or tweet the latest government failing to the world, each social media site provides a tool for terrorist organizations. Extremist use of social media is completely congruent with the design of the websites; the crux of the matter is in the messaging, not the methods.

INTERNATIONAL RESPONSES TO SOCIAL MEDIA CONTENT

The internet pioneers grew up in an anti-authoritarian era, from Civil Rights Movement through the end of the Vietnam War. The original designers of the internet saw the new technology as something that should be open and free to all.[46] Their design model succeeded, as the internet today reaches around the globe. The physical infrastructure of the internet brings with it the software and programs that ride on top of it, a concept the designers wanted, but failed to understand the second, third and fourth order affects that went with it.

Alongside the original intent of a free and open internet was the idea that the internet would be able to regulate itself.[47] The understanding was that government regulation of the internet would only get in the way of a free-flowing and open community. While this policy works for the standards and infrastructure practices of the internet, the private sector lacks the ability to police content and secure the internet.[48] Social media companies, like any other company, exist to make money. There are some security practices and content policing the companies can accomplish, but the motivating factor for companies is the bottom line on their

ledger. Adequately funding policing and security software is something private companies are not necessarily keen to do, despite the overall benefit to the internet as a whole, because the cost associated to them does not increase profit.[49] Even when policing and cleaning content on their website, companies lack any continuity between the major players.

In December 2011, India was at odds with the social media and internet companies over their refusal to, "screen derogatory material from their sites," over content insulting political leaders and religious figures.[50] In response to the issue, Facebook stated it would remove content that, "is hateful, threatening, incites violence or contains nudity," while Google (YouTube's parent company) replied it removes content when it, "violates local law and [our] own standards."[51] The sincerity of the companies' comments is questionable at best. Indian Telecommunications Minister Kapil Sibal pointed out the disconnect between western internet companies and their international hosts when he was told by the companies they, "were applying US standards to their sites."[52] This is something India and other countries do not accept.

Even within their own company, the standards applied to international partners differ greatly. In 2012, the British Association of Chief Police Officers requested YouTube remove 640 videos and 5 accounts that promoted terrorism.[53] YouTube agreed with the association, removed the videos and deleted the accounts; however, just because a request is made of YouTube does not mean the company will necessarily remove the video. Canada requested YouTube remove a video of a citizen urinating on a Canadian passport, YouTube denied the request; similarly, Pakistan requested removal of videos making fun of its military and senior officials, again the request was denied.[54] The disparity between requests made of the company and approval granted is staggering when looking at the countries making the request. YouTube

approved 93% of the American requests to remove content, while Hungary, Turkey and Russia did not have a single request partially or fully removed.[55]

The open internet model of private policing is not meeting countries' expectations. At present, social media companies are not capable of sufficiently controlling and monitoring content to the satisfaction of the countries in which they operate. Whether through unwillingness or inability, the situation forces nations to take the matter of controlling social media into their own hands. The wide variety of methods to control the content of social media highlights a paradoxical problem of controlling content or promoting freedom.

Some approaches rely on draconian blocks of specific websites or internet access in general. Another approach walks a fine-line of legislation to attempt to maintain openness yet still define the rules and regulations of what is acceptable on social media. A third innovative approach relies on the unique method of turning the tables against their adversaries by using social media against them.

When social media companies do not acquiesce to host government requests, the simplest method to police social media is not making it available to the populace. In a society with an open internet, this solution is nearly impossible due to constraint placed on government overreach. However, where countries do not necessarily need to worry about public opinion, authoritarian regimes or strong centralized governments, blocking the internet in general, blocking specific sites, or even blocking specific discussion topics is much easier.

An increasing number of countries are taking this route to control the internet and social media websites in their country. A study conducted by the Canadian International Development Research Centre discovered in 2002 that six countries were restricting access to the internet in their countries. In 2013, the number had increased to 26 countries out of 43 surveyed.[56] The

most draconian of censors is North Korea, where the regime has essentially blocked the internet from reaching inside the country. There is an intranet available within North Korean borders, but it is limited to roughly 30 sites and only an elite minority has access.[57] The most intriguing and advanced country utilizing blocks on social media is China. Eschewing the broad brush of blocking everything, the Chinese use a combination of controlling internet access into the country, blocking specific sites, and actively controlling content on websites within the country.

In what is known as the "Great Firewall of China," the Chinese government controls the internet access points to its country, with this power it is able to completely cutoff the world wide web to its citizens. Though it has not used such power countrywide, the ruling party has removed internet connectivity to sections of the country during times of civil unrest. In 2009, in response to an uprising by the indigenous Urumqi people, the ruling party shut down internet and telecommunication access to the Xinjiang province, home of the Urumqi.[58]

The Chinese government does not simply view control of the internet as an on/off valve; they also filter websites to prevent information from getting out and ideas from getting into the country. Internet service providers block Facebook and Twitter, preventing the companies from operating within China.[59] Just because China blocks Facebook and Twitter however, does not mean that China does not allow social media within its borders. The country developed its own social media websites that are allowed to operate, the most popular being Sina Weibo. The website provides China's internet users the same functionality as its western counterparts, but unlike Facebook and Twitter, the Chinese central government monitors and controls Sina Weibo for content, the third part of control in China's internet censorship triad.

Western social media companies tend to be reactive and rely on user reporting to police content, the Chinese government proactively monitors and removes content from websites it

finds inappropriate. As stated, the Chinese government has the ability to completely remove internet access to the entire country and specific provinces, but is also maintains the surgical ability to control websites' content without removing connectivity to the site altogether. To operate a social media website within China, the company must establish an internal censorship team that takes its order from the government.[60] In total, the Chinese government has over 2 million people called, "public opinion analysts," monitoring the internet and websites for anything critical to the ruling party or fomenting feelings of unrest.[61] The "analysts" play an intriguing game of cloak and dagger with the internet users within China trying to get information out.

After blind Chinese activist Chen Guangcheng escaped house arrest in 2012, the blogs in China lit up trying to push and pull information regarding Guangcheng. Initially, Chinese web censors blocked the name of Guangcheng in both Chinese and English letters; undeterred, users begin to use code words such as A Bing as a pseudonym for Guangcheng, the government adapted and A Bing was soon blocked.[62] The back and forth between the government and net users continued for days, with searches related to the movie, *Shawshank Redemption* being blocked as some used the prison escape movie to refer to Guangcheng. The speed at which the Chinese government censors and blocks web content is measured in minutes and hours compared to weeks and months of western companies. For reference, after a British court convicted Roushana Choudhry of stabbing a Member of Parliament over 5,000 videos of Anwar al-Awlaki's sermons remained accessible on YouTube.[63]

China's response to unwanted material on social media is as effective as it is draconian, but as an authoritarian government, the Chinese ruling party has that luxury. For societies that are more democratic and even those societies moving towards democracy, the use of such overt

censorship methods undermines their governance or political desires. What takes the place of physical censorship of social media is legislation aimed at curtailing the extreme uses of social media. Three examples with relatively unrelated governance structures and cultures, Mexico, United Arab Emirates, and United Kingdom, show how the use of legislation as a tool can decrease social media use by terrorists but is a slippery slope away from freedom of speech.

Unnerved by the upswing in drug trade violence in their country, the Mexican government began to crack down on messages within social media websites. After the drug cartels and organized crime began using social media to extort, harass, and in extreme cases murder those who oppose them, the Mexican government decided to step in and do something to curtail the violence.[64] The desire to get control of parts of the country back from the cartels led the Mexican government to take overreaching steps against online terror. The government arrested two individuals for, “sowing fear,” after they mistakenly posted to Twitter and Facebook news of a primary school in Veracruz under attack with children kidnapped.[65] Neither person was associated with a terror organization, but their arrest shows how some countries will take a wide berth with their legislation in order to try to keep the peace. When questioned on the incident, Veracruz Governor Javier Duarte tweeted, "I am a Tweeter by heart, I am in favor of freedom of speech but I also defend our right to live in tranquility and peace."[66] The legislation of content on websites is at best extremely difficult; Mr. Duarte adequately sums up the tug and pull between freedom and safety. In this specific case, after a large public outcry by human rights groups, the state dropped the case against the two individuals.[67]

Halfway around the world, another country struggles to find the balance between abridging speech and controlling content on social media. In 2011, the United Arab Emirates began enforcing legislation that made it illegal for individuals to spread rumors or false information that

could, "harm UAE society."[68] The interpretation of the law left users unsure as to what constituted content that could harm the society. Unabridged laws intent on controlling social media can lead nations to a point where they terrorize their own citizens.

In the UAE, the government arrested five bloggers for posting information suggesting democratic reforms in the country, yet allowed those who openly deride the activists to continue posting.[69] Are countries using these laws to stop extremists or simply control content within their own borders? Some intellectual latitude can be given regarding the UAE, hardly considered a bastion of Jeffersonian Democracy, but the line between freedom and safety is blurred even further when a similar issues arises in the United Kingdom.

"Free flow of information can be used for good, but it can also be used for ill," according to British Prime Minister David Cameron, responding to August 2011 riots in London.[70] The unrest, initially caused by London police fatally shooting of Mark Duggan during a police investigation, started as peaceful protests but eventually turned into riots across the city.[71] What caused the Prime Minister's comment on information flow was the use of Facebook and Twitter to organize and encourage the rioting. The government arrested individuals using social media and unlike the Mexico case study, was able to get a conviction on some of the individuals by linking their online activities to the physical violence on the streets.[72]

Even though the case of the rioters use of social media was not a terror organization, the subsequent legislation passed in the United Kingdom, and in France directly focusing curbing online content trumpeting terrorism. Both European nations have passed legislation that makes advocating or glorifying terrorism a criminal offense.[73] The prosecution of individuals using social media to encourage riots and the criminalization of speech glorifying terrorism come dangerously close to infringement of basic speech rights. Legislating social media use is a

difficult proposition as the previous case studies demonstrate. Instead of trying to merely control social media, what if countries utilized social media against extremists the same way it is used against them? Indonesia harnessed the power of social media by conducting a campaign against one of their most infamous terrorists.

Noordin Mohammad Top was one of the top members of Jemaah Islamiyah (JI), an Indonesian terror organization. The believed mastermind of the 2003 Marriott Hotel bombing in Jakarta, 2005 Bali bombing, and 2009 Ritz-Carlton and Hilton attacks in Jakarta, was a celebrity for the organization.[74] He formed an offshoot from JI in 2009, linked the group to Al Qae'da and posted the new group's ideologies on YouTube.[75]

Reportedly killed by authorities multiple times, the rumors of his death always proved greatly exaggerated. When Indonesian authorities finally surrounded and killed Noordin, before announcing his death to the press, they conducted a forensic autopsy on the body to be sure. Once confirmed, the police held a press conference announcing his death, yet also released details about the autopsy stating there was, "an anomaly in Noordin's anus…indicat[ing] that somebody had sodomized him."[76] The initial reporting by the press connected the dots laid out before them that Noordin was a homosexual, an affront to his organization, JI and Islam in general. The mainstream Indonesian media dropped the story the next day to cover an earthquake killing thousands in Sumatra, but social media sprung upon the story and would not let it go.[77]

Subsequent research reveals that the condition Noordin Top had was not linked to homosexual activity, it occurs naturally in about 3.5% of the population. What remains unknown is whether the autopsy doctor knew this information at the time of the press release and continued with the story or did not know from the outset.[78] Regardless of the details, the fact is

the state authorities released the rumor of Noordin Top's supposed homosexuality. The accusation stuck and online ridicule affected JI's credibility.

Unlike the mainstream media, the limits to which social media goes are much less bounded. Hyperbole on social media is a way to garner more attention. As such, the stories about Noordin that spread on social media were the most outlandish ones. When JI's own spiritual leader calls for the stoning of homosexuals, much of the groups' gravitas gained from their bombings is lost.[79] Questions began to arise about the sexuality of JI's leadership, if such a high ranking and influential member of the group was gay, how could the other leaders not know about it? Were they also gay? The rumors on social media and mockery on YouTube eviscerated JI's claims of being an ideological group.

The whisper campaign undertaken by the Indonesian government is only one way that countries are attempting to control or use social media to their benefit. The developers of the internet imagined it as an open, self-regulating cyber reality. The internet is indeed open, but where countries were aloof to the openness in the past, they are taking actions to control it in the present and into the future. The inability or inaction of private social media companies to redress host nation concerns only exacerbates the length to which governments will go to control internet content within their borders. Whether the actions are outright censorship and physical control, legislation balancing security and freedom or irregular, by utilizing whisper campaigns, each country must what and how appropriately to control social media content—including the United States.

US RESPONSE TO SOCIAL MEDIA AND THE WAY AHEAD

There is a wide range of international responses to policing and controlling content on social media. Where does the United States fit into the mix? Where does the "city on the hill" stand with respect to social media, terrorism and control and what is the way forward?

The United States recognizes it is in a difficult information campaign with terror and extremist organizations; social media is one of the main battlefields. America understands it cannot control the internet completely but it needs to work within its own system and with other nations to balance the freedom of its people with the responsibility of assuring their safety. The United States needs to find the balance between active denial, passive coercion and situation awareness of social media to best protect the citizenry while maintaining their freedoms.

America has come a long way since the Clinton Administration's economic focus on internet activity. Leery of interfering with the open internet and the consequences it could have on a booming economy, President Clinton chose a former college activist to oversee the commercialization of the internet. Ira Magaziner, following the model of those before him believed the government was a poor choice to police the internet. To Magaziner, and many others at the time, the best way to police the internet was self-regulation and industry best practices, and keeping any central control at a minimum.[80] The self-regulation of the internet did see breakthrough in economic activity. Viewing security as only an afterthought though brought America to the difficult situation of controlling the internet today.

As it currently stands, the United States is still not very convincing it has a fully grasped the information struggle it is in against extremist and terror organizations. Secretary of Defense Donald Rumsfeld was very blunt in his assessment of the information war in 2006. "I would probably say we deserve a 'D' or a 'D-plus'," he further elaborated the difficulty of the

information war, “I’m not going to suggest its easy, but we have not found the formula as a country for countering the extremists’ message.”[81] When Rumsfeld made these comments, the social media explosion was just beginning; the difficulty in countering the messages in the social media age is much greater now than it was in 2006.

The Obama Administration took a good positive step by admitting to the American people eradication of extremist messaging is not possible. When referencing the dangers of terrorism, the National Security Strategy states, “we [also] recognize that we will not be able to deter or prevent every single threat.”[82] The administration further set expectations in the National Strategy for Counterterrorism by recognizing, “The United States alone cannot eliminate every terrorist or terrorist organization…” which also codifies the need for allies in this struggle.[83] Learning from mistakes and success of other countries and being able to apply them to the landscape of the United States is paramount.

There is no single magic tonic or silver bullet to solve the issue of regulating extremism on social media. Like Pandora's Box, the world cannot close the internet now that it is open. The United Stated needs to look across the world for best practices and apply multiple and varied solutions to best handle social media extremism. A special report from the Australian Strategic Policy Institute outlines a three-prong strategy on how to counter internet extremism. Through a combination of hard strategy (banning websites), soft strategy (messaging on the internet) and monitoring content for intelligence purposes the United States can use this formula on social media as well.[84] The government cannot solely assume these three avenues, nor can they only be the responsibility of the private industry. Looking to the Indian strategy, the government and private industry must coordinate actions together in order to gain the most effective and efficient

method of combating extremist messages.[85] Without coordination, the two entities run the risk of actions being at odds with one another.

Of the three methods to the Australian model, the most difficult for the United States is the hard-line approach of actively denying social media to extremists. As the "leader of the free world," America must ensure it does not do anything regarding infringement of rights in the open so that the public is aware. The government needs to understand the mood of the country before enacting any legislation seen to take away the privacy of the populous. While it is true that Americans are willing to give up some of their freedoms in times of national crisis, such as 9/11, the pendulum inevitably swings back the other way.[86]

This does not mean that the government and private business cannot enact policies and legislation to prevent extremism from entering social media; it means the public must see government transparency when doing so. There are already programs on social media that monitor for and remove content deemed inappropriate. If YouTube's record of removing pornography, nudity, and copyright infringements are any indication, there is little reason extremist videos cannot fall under the same scrutiny.[87] Congress needs to pressure social media companies to start acting responsibly in the fight against extremist messaging. In the past companies acted as passive bystanders; however, enacting fines or mandating a more active monitoring program against Facebook, Twitter, and YouTube would spur action.[88] Affecting the bottom line of private industry will do more for compliance than appealing to their patriotic duty.

There has already been some progress made through technology. Facebook is developing facial recognition software that is currently accurate at a 97.25% rate, only slightly behind a human success rate of 97.53%.[89] Theoretically, a company like YouTube could utilize the facial recognition software to search for symbols prevalent in extremist videos, such as "watermarks"

in the corner of violent jihadist postings.[90] YouTube could either automatically remove the video or quarantine the video until a monitor is able to view the content to validate its legitimacy.

The technology solutions only deal with content, a second part to active denial is being able to prosecute those placing the content online or promoting the extremist ideologies. The successful criminal case against Tarek Mehanna shows the administration is serious about consequences for aiding extremists online. The government successfully argued that Mehanna, through translation of terrorist materials and actively discussing the possibility of a terror attack on a US mall, was "material support," to terrorists, in this case Al Qaeda.[91] As expected and with valid counterpoints, civil liberty groups are appealing the case. They argue Mehanna's actions were not supporting Al Qaeda and disagree with the extension of the definition of, "material support," to include online actions.[92]

The freedom or security argument will remain and is most difficult part in active denial of social media websites to extremist ideologies. Whether there is outright banning via software or legislative issues of free speech, the use of active denial requires proactive responses from the government. The softer approach, used in tandem with active denial, is about counter-messaging the extremists on social media.

The internet is a location more understood and traversed by younger generations. This is not to say older generations are not capable of understanding the nuances of social media, but when a generation grows up in the age of Web 2.0, they are more adept at its use and understand it deeper. The soft strategy of passive coercion, providing a counter-message to extremism seeks to stop those who would espouse extreme values on social media before they ever become a problem.[93]

Dating back to the Cold War Era, the United States had an agency that controlled the messaging to the outside world on US policy. Created by President Dwight Eisenhower in 1953 the United States Information Agency (USIA) had four main missions:

> 1) Explain and advocate US policies in terms that are credible and meaningful in foreign cultures
> 2) Provide information about the official policies of the United States and about the people, values and institutions that influence those policies
> 3) Bring the benefits of international engagement to American citizens and institutions by helping them build long-term partnerships with overseas counterparts
> 4) Advise the President and policy makers on way which foreign attitudes will have bearing on the effectiveness of US policies[94]

Though the intent of the agency focused on countering communist propaganda while promoting US propaganda, the essential qualities of USIA fall directly in line with the soft strategy of counter-messaging on social media. The genesis of the organization began with the Smith-Mundt commission, which wanted to combat, "weapons of false propaganda and misinformation," against foreign populations.[95] The words can be transposed directly to what needs to be done in social media to counter the extremists. A recreation of USIA with a modern spin for the technology of today could vastly improve the US position on social media in the information age.

A second method of soft strategy is to draw an example from the Indonesians and the whisper campaign they conducted post mortem on Noordin Top. The United States does have a history of ridicule and attempting to emasculate terrorists via social media and the internet, but it needs to conduct more operations. There needs to be more action taken like the example of Abu Musab al-Zarqawi, the former leader of Al Qaeda in Iraq.

Prior to his death, many videos on YouTube and the internet showed Zarqawi as a capable fighter against the Americans and coalition. However, when US troops captured the

unedited video of Zarqawi during a raid, they took the video to the internet to discredit him. Instead of a capable and diligent operator, the video showed Zarqawi unable to fix a simple jam in his rifle, the video also pointed out his hypocrisy of western culture when he was shown wearing American sneakers.[96] The posted video by the Americans further ridiculed his organization; displaying one of his fighters foolishly burning his hand on the just fired barrel of a machine gun, a mistake not made by an individual with any live fire experience.[97]

The United States has already used passive coercion and soft strategy in the Cold War through USIA. The power of messaging has not changed in the decades, even though the medium has. New generations grow up understanding social media, how to navigate through it and how to get and post information. Passive coercion works to ensure there is a counter-message for would-be extremists, a positive message on social media, and not simply those spouting extremism and hate.

The undercurrent of both active denial and passive coercion needs to be a situational awareness of what is going on in social media. The internet, especially with the advent of Web 2.0 and user driven content, has become a goldmine for open source intelligence gathering. When an individual or group can place any information they desire out in the open, that information becomes readily available to those who use it for nefarious reasons. The website PleaseRobMe.com shows people the vulnerability of over-sharing. How a simple tweet about how you cannot wait to go to Las Vegas in two weeks informs the whole world when your home is going to be empty.[98]

The same sort of open source intelligence can be used against extremist individuals or groups over-sharing on social media turning digital missteps into actual arrests or targetable information on a battlefield. The NYPD is already using this sort of open source intelligence on

gangs. With social media and Web 2.0 comes an, "irresistible urge," of users to post and brag about their exploits, exactly what rival gangs began doing in New York City.[99] Often times, the posts from extremists involve boasting about illegal activities that they believe they have "gotten away with." Gang members in New York City posted details about rival gang fights and the activities they committed. The NYPD, over a three-year period of data mining, was able to create a large portion of the gang networks through individuals' posts, resulting in 49 arrests on homicide and other gang-related crimes.[100]

Maintaining situational awareness of social media is not only valuable to catch extremists in the acts of committing or planning violence, but also is able to locate and identify key members, monitor them and ultimately map out an entire organization. This technique displayed its validity against Al Qaeda affiliates in Singapore, Morocco and the Maghreb. Instead of attacking and arresting cells when they were first identified through social media, the authorities waited to allow the network to further expand and only then came down upon the entire operation.[101]

Crowdsourcing, another name for the open source intelligence gathered from social media and Web 2.0 content, is an operation that has shown its value in law enforcement and counterterrorism activities. The amount of information available on the internet and in social media is vast, there needs to be adequate resources allocated to avoid missing possible information leads. Social media is a double-edged sword, it allows extremist groups a platform to gain access to the population, but it also provides law enforcement and military intelligence access to the extremist organizations as well.

The United States needs to get its social media policing policy right, it does not need to be perfect, and there will be proverbial bumps in the road. Above all, it must balance the

freedoms synonymous with America to the reality of extremists throughout the world today. Through a multifaceted policy of hard power, coercion and situational awareness on the internet the correct solution is possible. America does not have to fight the battle alone. By looking outward to allies and other nations' policies and being able to respond to internal and external influences the United States can stay ahead of the extremists on the battlefield of social media information.

CONCLUSIONS

Technological advances on the internet, to include Web 2.0 and the social media sites that utilize the programming, have opened up internet content to the common user, not just website designers. Social media today is home to almost anything the user can imagine, sharing photographs, interests, reunions, political statements, vacation plans, the limit to what people use social media for lies with the individual, not the program.

Social media exists for the extremist the same way it exists for the everyday user, neither evil nor benevolent. Social media websites are simply a method extremists use to conduct a myriad of organizational functions. Facebook, Twitter, or YouTube, are the most popular social media sites today, but that does not mean they will stay such. Tumblr, LinkedIn, Google+, and Instagram are all social media sites growing in popularity. It is imperative for counter-terror efforts to acknowledge and keep abreast of new advances in social media.[102] The case studies showing extremist use of Facebook, Twitter and Facebook are the current reality, however, they are not a status quo. If anything, history teaches that change is inevitable. Nations must be proactive in addressing the issues before the next Anwar al-Awlaki makes a name for themselves on one of these sites. The uses for social media and extremism are known, experts need to start

thinking how those methods can be translated to the new social media sites beyond those addressed.

The rise of more social media is accompanied by extremist groups' penchant to change their current online tactics. Aware of government conducting intelligence on social media sites, extremists have begun using operational security to avoid detection as long as possible. Transcripts from jihadist forums indicate instructions of Facebook use, to include not using your real photograph, changing passwords often, not using the same password for different social media sites and using fictional data for e-mail and profile information.[103] Countries must be prepared for the changing tactics of extremists on social media and the internet.

Multiple options exist for controlling and policing content throughout the world. The range extends from strict control of all aspect of social media and the internet, like North Korea, to allowing a complete, open and unfettered access to the internet. Nations can choose to utilize the internet for their own purposes as well, turning the table on extremist individuals and groups. Government type and how much authority the central government has to infringe on freedoms weigh heavily on the approach used to police social media. The more authoritarian governments, such as China, utilize a harsher stance towards an open internet. For a democratic country like the United States, a balanced approach is necessary to optimize policing social media with the principles of limited government interference.

There is no single answer to policing internet content given today's current infrastructure on the World Wide Web. The balanced approach of the United States needs to include elements of hard power, soft power and open source intelligence on social media. There is no static balance between each approach either, external and internal forces affect how much or little of each option can be exercised at any given time. The United States has shown both domestically

and internationally it has the ability to do each of the three elements, what it needs to focus on is flexing between each of them. The situation with social media and the internet is always changing and requires proactive responses from not only the government and but also private industry.

The World Wide Web is here to stay; social media is here right now and likely for some time to come. Extremist social networking has evolved from face-to-face interactions in back alleys and marketplaces to digitally across the globe in a matter of seconds. Bad actors and elements are adapting and utilizing social media for their own agenda and purposes. The countries of the world need to adapt to the new methods employed on social media. By having a greater understanding of social media and how it is used by those who would do them harm, they can be proactive in stopping them before it gets out of control.

1 Sly and Ramadan, "Syrian Extremists" http://www.washingtonpost.com/blogs/ worldviews/wp/2014/02/28/syrian-extremists-amputated-a-mans-hand-and-live-tweeted- it/
2 Ibid.
3 Ibid.
4 Kohlmann, House Testimony "The Anti-social Network" 2.
5 Leyden, Joel, "Al Qaeda: The 39 Principles of Holy War."
6 Ibid.
7 Ibid.
8 Coll, and Glasser, "Terrorist Turn to the Web as a Base of Operations."
9 Freeman and Simmons eds., "Special Issue: Social Media in Jihad and Counterterrorism," 23.
10 Dean, Bell, and Neumann "The Dark Side of Social Media," 112.
11 Veerasamay and Grobler "Terrorist use of the Internet," 261.
12 Ibid.
13 Pradhan, "Internet, Social Media and Terrorism," 367-368.
14 Public Intelligence "DHS Terrorist Use of Social Networking Facebook Case Study." http://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook- case-study/
15 eBIZ|MBA. "Most Popular Websites: March 2014." http://www.ebizmba.com/articles/most- popular-websites
16 eBIZ|MBA. "Most Popular Websites: March 2014." http://www.ebizmba.com/articles/most- popular-websites
17 ElectronicResistance, "Hezbollah|Electronic Resistance Introduction," http://www.youtube.com/user/berjaoui0/featured
18 Aryan Nation World Headquarters, "The Shadow of He to Come," http://www.youtube.com/watch?v=zqGgv-9UjJ8&list=UUDBaIeSH2mV-7sOd9Q8D5Pg
19 Ibid.
20 Pradhan, "Internet, Social Media and Terrorism," 371.
21 Kohlmann, House Testimony "The Anti-social Network" 6.
22 Ibid.
23 Ibid.
24 YouTube, "Terror and Social Media."
25 http://www.youtube.com/results?search_query=how+to+clean+an+ak-47&sm=3
26 http://www.youtube.com/results?search_query=how+to+fundraise+money&sm=1
27 Dean, Bell, Neumann "The Dark Side of Social Media," 112.
28 Ibid.
29 Dean, Bell, Neumann "The Dark Side of Social Media," 109-110.
30 Lachow and Richardon, "Terrorist Use of the Internet: The Real Story," 100.
31 Hedges, Review of *The Death and Life of American Journalism,"* http://www.truthdig.com/arts_culture/ item/chris_hedges_on_the_death_and_life_of_amer ican_journalism_20100226
32 Al-Shishani, "Taking al-Qaeda's Jihad to Facebook." 3.
33 Ibid, 4.
34 eBIZ|MBA. "Most Popular Websites: March 2014." http://www.ebizmba.com/articles/most- popular-websites
35 Dean, Bell, Neumann "The Dark Side of Social Media," 110.
36 Kotenko, "According to a New Report, Twitter is a Breeding Ground for Terrorism and Hate Speech." http://www.digitaltrends.com/social-media/online-hate-statistics-up-by-30-percent-says-report-but-theres-a-new-app-designed-to-get-it-under-control/#!z3Gwn
37 Koh, "African Militants Turn More to Social Media.":://online.wsj.com/article/ SB10001424052702304713704579091720477473610.html
38 Chiluwa and Adegoke, "Twittering the Boko Haram Uprising in Nigeria," 85.
39 Ibid., 91.
40 Ibid.
41 Ibid., 95.
42 Koh, "African Militants Turn More to Social Media.":://online.wsj.com/article/ SB10001424052702304713704579091720477473610.html
43 YouTube, "Terror and Social Media."

44 Dean, Bell, Neumann "The Dark Side of Social Media," 110.
45 Ibid., 111.
46 Lewis, "Sovereignty and the Role of Government in Cyberspace," 55-58.
47 Ibid., 57-58.
48 Ibid.
49 Ibid.
50 Nessman, "Facebook Faces Possible Censorship in India." http://www.huffingtonpost.com/2011/12/06/facebook-google-censorship-india_n_1131206.html#
51 Ibid.
52 Ibid.
53 "Google Removes 640 Videos from YouTube Promoting Terrorism," http://www.telegraph.co.uk/technology/google/9337993/Google-removes-640-videos-from-YouTube-promoting-terrorism.html
54 Ibid.
55 Ibid.
56 Ibid.
57 "North Korea," https://opennet.net/research/profiles/north-korea.
58 Rauhala, "China's Great Firewall Won't Be Touched by Beijing's New Reforms."
59 Cross, *Bloggerati Twitterati*, 113.
60 Simonite, "Reading the Tea Leaves of Censorship," 20.
61 Hunt and Xu, "China 'Employs 2 Million to Police Internet," http://www.cnn.com/2013/10/07/world/asia/china-internet-monitors/
62 McDonald and Tang. "Chen Guangcheng, Escaped Blind Activist, Censored by Chinese Government." http://www.huffingtonpost.com/2012/05/01/chen-guangcheng-censor_n_1468823.html#
63 "Google Removes 640 Videos from YouTube Promoting Terrorism. http://www.telegraph.co.uk/technology/google/9337993/Google-removes-640-videos-from-YouTube-promoting-terrorism.html
64 Logan, "Mexico: Death by Social Media." http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=133074&lng=en
65 Hernandez, "Terrorism Charges for 2 in Mexico Who Spread Attack Rumor on Twitter, Facebook." http://latimesblogs.latimes.com/laplaza/2011/09/twitter-tweets-veracruz-mexico-terrorism-drug-war-censorship-rumors.html
66 Ibid.
67 Logan, "Mexico: Death by Social Media." http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=133074&lng=en
68 Hibbard, "UAE: Tweeting Rumors can Land You Three Years in Jail." http://www.huffingtonpost.com/2011/08/18/uae-tweeting-rumors-can-result-in-jail-time_n_929351.html
69 Cassel, Matthew. "Trial of UAE Bloggers Set to Resume." http://www.aljazeera.com/news/middleeast/2011/07/2011717213325459958.html
70 Halliday, "David Cameron Considers Banning Suspected Rioters from Social Media." http://www.theguardian.com/media/2011/aug/11/david-cameron-rioters-social-media?INTCMP=ILCNETTXT3487
71 "Mark Duggan shooting: Bullets results 'within 24 hours'." http://www.bbc.co.uk/news/uk-england-london-14443311
72 Freeman and Simmons eds., "Special Issue: Social Media in Jihad and Counterterrorism" 36.
73 Schmitt, "Terrorism and the First Amendment." *The Weekly Standard* 17, no. 18, 1.
74 Bernardi, Cheong, Lundry, and Ruston, *Narrarative Landmines: Rumors, Islamist Extremism, and the Struggle for Strategic Influence*, 101.
75 Ibid., 105.
76 Ibid., 106.
77 Ibid., 108.
78 Ibid., 111
79 Ibid., 106.
80 Lewis, "Sovereignty and the Role of Government in Cyberspace," 58.

81 Robert, “Rumsfeld: US Losing War of Ideas.” http://www.cbsnews.com/news/rumsfeld-us-losing-war-of-ideas/
82 *The National Security Strategy of the United States.* 10.
83 *The National Strategy for Counterterrorism*, 6.
84 Bergin, Osman, Ungerer; and Yasin "Countering Internet Radicalization in Southeast Asia," *Australian Strategic Policy Institute*, 12.
85 Pradhan, "Internet, Social Media and Terrorism," 363.
86 Enton, "No Patriot Act II," http://www.theguardian.com/commentisfree/2013/may/03/americans-choose-liberties-over-security-after-boston
87 Kohlmann, House Testimony "The Anti-social Network" 10.
88 Ibid.
89 Simonite, "Facebook Creates Software that Matches Faces Almost as Well as You Do," http://www.technologyreview.com/news/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/.
90 Kohlmann, House Testimony "The Anti-social Network" 11.
91 Schmitt, "Terrorism and the First Amendment." *The Weekly Standard* 17, no. 18, 1.
92 Ibid.
93 Bergin, Osman, Ungerer; and Yasin "Countering Internet Radicalization in Southeast Asia," *Australian Strategic Policy Institute*, 17-18.
94 Chodkowski, "Fact Sheet: United States Information Agency." http://americansecurityproject.org/featured-items/2012/fact-sheet-the-united-states-information-agency, 2-6.
95 Ibid., 2.
96 Bernardi, Cheong, Lundry, and Ruston, *Narrarative Landmines: Rumors, Islamist Extremism, and the Struggle for Strategic Influence*, 129.
97 Ibid.
98 Kim, "PleaseRobMe.com Posts When You Are Not at Home."http://www.sfgate.com/crime/article/PleaseRobMe-com-posts-when-you-re-not-at-home-3272742.php
99 Freeman and Simmons eds., "Special Issue: Social Media in Jihad and Counterterrorism," 70.
100 Ibid.
101 Ibid., 71.
102 Pradhan, "Internet, Social Media and Terrorism," 371.
103 Public Intelligence "DHS Terrorist Use of Social Networking Facebook Case Study." http://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook- case-study/

Bibliography

Al-Shishani, Murad Batal. "Taking al-Qaeda's Jihad to Facebook." *Terrorism Monitor* 8, no. 5 (4 February 2010): p. 3-4.

Aryan Nations World Headquarters. "The Shadow of He to Come." http://www.youtube.com/watch?v=zqGgv-9UjJ8&list=UUDBaIeSH2mV-7sOd9Q8D5Pg (accessed 28 March 2014).

Bergin, Anthony, Sulastri Bte Osman, Carl Ungerer and Nur Azlin Mohammad Yasin. "Countering Internet Radicalization in Southeast Asia." *Australian Stategic Polcy Institute*, March 2009, issue 22.

Bernardi, Daniel Leonard, Pauline Hope Cheong, Chris Lundry, and Scott W. Ruston. *Narrarative Landmines: Rumors, Islamist Extremism, and the Struggle for Strategic Influence.* New Brunswick NJ: Rutgers University Press, 2012.

Carafano, James Jay. *Wiki at War: Conflict in a Socially Networked World.* College Station TX: Texas A&M University, 2012.

Cassel, Matthew. "Trial of UAE Bloggers Set to Resume." *AlJazeera.com* July 18, 2011. http://www.aljazeera.com/news/middleeast/2011/07/201171721332545995 8.html

Chodkowski, William M. "Fact Sheet: United States Information Agency." *American Security Project*, http://americansecurityproject.org/featured-items/2012/fact-sheet-the-united-states-information-agency/ (accessed 26 March 2014)

Chiluwa, Innocent and Adetunji Adegoke, "Twittering the Boko Haram Uprising in Nigeria: Investigating Pragmatic Acts in the Social Media." *Africa Today* 59, no. 3 (Spring 2013): 82-102.

Coll, Steve and Susan B. Glasser. "Terrorists Turn to the Web as a Base of Operations." *The Washington Post*, 7 August 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html

Cross, Mary. *Bloggerati Twitterati: How Blogs and Twitter are Transforming Popular Culture.* Santa Barbara CA: Praeger Publishing, 2011.

Dartnell, Michael Y. *Insurgency Online: Web Activism and Global Conflict.* Buffalo NY: University of Toronto Press, 2006.

Dean, Dr. Geoff, Peter Bell and Jack Neuman. "The Dark Side of Social Media: Review of Online Terrorism." *Pakistan Journal of Criminology* 3, no. 3 (January 2012): 107-126.

eBIZ|MBA. "Most Popular Websites: March 2014." http://www.ebizmba.com/articles/most-popular-websites (accessed 25 March 2014).

ElectronicResistance. "Hezbollah|Electronic Resistance Introduction." http://www.youtube.com /user/berjaoui0/featured (accessed 28 March 2014).

Enton, Harry J. "No Patriot Act II: Americans Choose Civil Liberties over Security Laws." *TheGuardian.com*, 3 May 2013. http://www.theguardian.com/commentisfree /2013/may/03/americans-choose-liberties-over-security-after-boston (accessed 7 April 2014).

Freeman, Michael and Anna Simmons eds., "Special Issue: Social Media in Jihad and Counterterrorism." *Combating Terrorism Exchange* 2, no. 4 (November 2012).

"Google Removes 640 Videos from YouTube Promoting Terrorism." *The Telegraph*, 18 June 2012. http://www.telegraph.co.uk/technology/google/9337993/Google-removes-640-videos-from-YouTube-promoting-terrorism.html

Halliday, Josh. "David Cameron Considers Banning Suspected Rioters from Social Media." *Theguardian.com* August 11, 2011. http://www.theguardian.com/media/2011/aug /11/david-cameron-rioters-social-media?INTCMP=ILCNETTXT3487 (accessed 3 April 2014).

Hedges, Chris. Review of *The Death and Life of American Journalism: The Media Revolution that will Begin the World Again.* McChesney, Robert W. and Charles Nichols. http://www.truthdig.com/arts_culture/item/chris_hedges_on_the_death_and_life_of_amer ican_journalism_20100226 (acccessed 29 March 2014).

Hernandez, Daniel. "Terrorism Charges for 2 in Mexico Who Spread Attack Rumor on Twitter, Facebook." *Los Angeles Times* September 1, 2011. http://latimesblogs.latimes.com/ laplaza/2011/09/twitter-tweets-veracruz-mexico-terrorism-drug-war-censorship-rumors.html

Hibbard, Laura. "UAE: Tweeting Rumors can Land You Three Years in Jail." *HuffingtonPost*, 18 August 2011. http://www.huffingtonpost.com/2011/08/18/uae-tweeting-rumors-can-result-in-jail-time_n_929351.html

Hunt, Katie and CY Xu. "China 'Employs 2 Million to Police Internet'." *CNN.com* October 7, 2013. http://www.cnn.com/2013/10/07/world/asia/china-internet-monitors/ (accessed 2 April 2014).

Kim, Ryan. "PleaseRobMe.com Posts When You Are Not at Home." *SFGate.com* February 18 2010. http://www.sfgate.com/crime/article/PleaseRobMe-com-posts-when-you-re-not-at-home-3272742.php (accessed 6 April 2014).

Koh ,Yoree. "African Militants Turn More to Social Media." *The Wall Street Journal*, 22 September 2013. http://online.wsj.com/article/SB10001424052702304713704579091720477473610.html

Kohlmann, Evan F. Testimony to the House, Committee on Homeland Security. *The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations,* December 6, 2011.

Kotenko, Jam. "According to a New Report, Twitter is a Breeding Ground for Terrorism and Hate Speech." *Digital Trends* 10 May 2013. http://www.digitaltrends.com/social-media/online-hate-statistics-up-by-30-percent-says-report-but-theres-a-new-app-designed-to-get-it-under-control/#!z3Gwn

Lachow, Irving and Courtney Richardon. "Terrorist Use of the Internet: The Real Story." *Joint Forces Quarterly* 45. (2d Quarter 2007): 100-103.

Lewis, James. "Sovereignty and the Role of Government in Cyberspace." *Brown Journal of World Affairs* 16, no. 2 (Spring/Summer 2010): 55-65.

Leyden, Joel. "Al Qaeda: The 39 Principles of Holy War." *Israel News Agency*, 4 September 2003. http://www.israelnewsagency.com/Al-Qaeda.html (Accessed 7 March 2014)

Logan, Samuel. "Mexico: Death by Social Media." *ISN ETH Zurich* September 28, 2011. http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=133074&lng=en (accessed 2 April 2014).

"Mark Duggan shooting: Bullets results 'within 24 hours'." *Bbc.co.uk* August 8, 2011. http://www.bbc.co.uk/news/uk-england-london-14443311 (accessed 3 April 2014).

McDonald, Joe and DiDi Tang. "Chen Guangcheng, Escaped Blind Activist, Censored b Chinese Government." *Associated Press,* 1 May 2012. http://www.huffingtonpost.com/2012/05/01/chen-guangcheng-censor_n_1468823.html#

Nessman, Ravi. "Facebook Faces Possible Censorship in India." *HuffingtonPost*, 12 June, 2011. http://www.huffingtonpost.com/2011/12/06/facebook-google-censorship-india_n_1131206.html#

Nacos, Brigitte L., Yaeli Bloch-Elkon and Robert K. Shapiro. *Selling Fear: Counterterrorism, the Media, and Public Opinion.* Chicago IL: University of Chicago Press, 2011.

"North Korea." *OpenNet Initiative.* https://opennet.net/research/profiles/north-korea (accessed 1 April 2014).

Pradhan, Lt Col Sushil. "Internet, Social Media and Terrorism." *Journal of the United Service Institution of India.* 141 no. 585 (July-September 2011): 366-374.

Public Intelligence. "DHS Terrorist Use of Social Networking Facebook Case Study." http://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/ (accessed 25 March 2014).

Rauhala, Emily. “China’s Great Firewall Won’t Be Touched by Beijing’s New Reforms.” *Time*, November 19, 2013.

Robert, Joel. “Rumsfeld: US Losing War of Ideas.” *CBSNews.com* March 27, 2006. http://www.cbsnews.com/news/rumsfeld-us-losing-war-of-ideas/

Schmitt, Gary. "Terrorism and the First Amendment." *The Weekly Standard* 17, no. 18 (12 January 2012).

Seib, Philip and Dana M. Jubanek. *Global Terrorism and New Media: The post-Al Qaeda Generation.* New York NY: Routledge, 2011.

Simonite, Tom. "Reading the Tea Leaves of Censorship." *MIT Technology Review* 116, no. 4 (July-August 2013): 20.

Simonite, Tom. "Facebook Creates Software that Matches Faces Almost as Well as You Do." *MITTechnologyReview.com* 17 March 2014, http://www.technologyreview.com/news/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/ (accessed 5 April 2014).

Sly, Liz and Ahmed Ramadan. "Syrian Extremists Amputated a Man's Hand and Live Tweeted it." *The Washington Post*, 28 February 2014. http://www.washingtonpost.com/blogs/worldviews/wp/2014/02/28/syrian-extremists-amputated-a-mans-hand-and-live-tweeted-it/

"Terror and Social Media." YouTube video, 5:50, posted by "CNN" April 27, 2013. http://www.youtube.com/watch?v=3DILJOvrA-A

The National Strategy for Counterterrorism. Washington DC: The White House, June 2011.

The National Security Strategy of the United States. Washington DC: The White House, May 2010.

Thompson, Robin. "Radicalization and the Use of Social Media." *Journal of Strategic Security.* 4, no. 4 (2011): 167-190.

Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges.* Washington DC: United States Institute of Peace Press, 2006.